

## A CASE FOR COLLABORATION IN COUNTERING TERROR

BY

COLONEL KATHLEEN A. GAVLE  
United States Army

### DISTRIBUTION STATEMENT A:

Approved for Public Release.  
Distribution is Unlimited.

USAWC CLASS OF 2009

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.



U.S. Army War College, Carlisle Barracks, PA 17013-5050



The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. <b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b>					
1. REPORT DATE (DD-MM-YYYY) 26-03-2009		2. REPORT TYPE Strategy Research Project		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE  A Case for Collaboration in Countering Terror				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)  Colonel Kathleen A. Gavle				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Professor Douglas Wake Department of National Security and Strategy				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <p>The best way to prevent another terrorist attack on the United States is to blend the best practices of the nation's law enforcement and military intelligence communities to avoid the seams or gaps that could result in any preventable attack. This project provides a broad overview of the national security and intelligence perspective of terrorism prior to 9/11, emphasizing the fault lines generally blamed for 9/11 and demonstrating the need for collaboration between law enforcement and military intelligence. It then examines some of the key reforms after 9/11 that addressed critical gaps in intelligence efforts. The paper provides three case studies to highlight the effectiveness of blending law enforcement and military intelligence capabilities to counter terrorism. The analysis concludes with the recommendation that these best practices become the norm for the national effort against terrorism and that existing obstacles to such interagency collaboration are critically examined for change as necessary to improve effectiveness. In doing so, the national security apparatus will gain the skills and flexibility that will not only prevent future terrorist attacks but might also help us recognize and counter the next adaptive threat on the horizon.</p>					
15. SUBJECT TERMS Special Operations, Law Enforcement, Military Intelligence					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT  UNLIMITED	18. NUMBER OF PAGES  30	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code)







USAWC STRATEGY RESEARCH PROJECT

**A CASE FOR COLLABORATION IN COUNTERING TERROR**

by

Colonel Kathleen A. Gavle  
United States Army

Professor Douglas Wake  
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College  
CARLISLE BARRACKS, PENNSYLVANIA 17013







## **ABSTRACT**

AUTHOR: Colonel Kathleen A. Gavle  
TITLE: A Case for Collaboration in the War on Terror  
FORMAT: Strategy Research Project  
DATE: 26 March 2009      WORD COUNT: 5,279      PAGES: 30  
KEY TERMS: Special Operations, Law Enforcement, Military Intelligence  
CLASSIFICATION: Unclassified

The best way to prevent another terrorist attack on the United States is to blend the best practices of the nation's law enforcement and military intelligence communities to avoid the seams or gaps that could result in any preventable attack. This project provides a broad overview of the national security and intelligence perspective of terrorism prior to 9/11, emphasizing the fault lines generally blamed for 9/11 and demonstrating the need for collaboration between law enforcement and military intelligence. It then examines some of the key reforms after 9/11 that addressed critical gaps in intelligence efforts. The paper provides three case studies to highlight the effectiveness of blending law enforcement and military intelligence capabilities to counter terrorism. The analysis concludes with the recommendation that these best practices become the norm for the national effort against terrorism and that existing obstacles to such interagency collaboration are critically examined for change as necessary to improve effectiveness. In doing so, the national security apparatus will gain the skills and flexibility that will not only prevent future terrorist attacks but might also help us recognize and counter the next adaptive threat on the horizon.







## A CASE FOR COLLABORATION IN THE WAR ON TERROR

Since the mid-1960s, international terrorism has been a national security threat to the United States. While the Cold War dominated American policies and processes, international terrorist attacks against Americans increased in number and scope through September 11, 2001 (9/11), when the threat became very real for the average American. Since 9/11, counterterrorism has become a primary effort for the country's national security apparatus, with the objective of preventing any other terrorist attacks.

The most important tool for accomplishing this objective is intelligence. The intelligence community has undertaken a number of reforms and efforts to improve its support of the nation's counterterrorism goal, and the fact that there have been no attacks on United States soil since 9/11 suggests they have been generally successful. We need to avoid overconfidence and complacency, however, as we move further away from the emotion and devastation of 9/11. This project contends that the best way to prevent another terrorist attack is to blend the best practices of the nation's law enforcement and military intelligence communities to avoid the seams or gaps that could result in any preventable attack. It provides a broad overview of the national security and intelligence perspective of terrorism prior to 9/11, emphasizing the fault lines generally blamed for 9/11 and demonstrating the need for collaboration between law enforcement and military intelligence. It then examines some of the key reforms after 9/11 that addressed critical gaps in intelligence efforts. The paper provides three case studies to highlight the effectiveness of blending law enforcement and military intelligence capabilities to counter terrorism. The analysis concludes with the recommendation that these best practices become the norm for the national effort



against terrorism and that existing obstacles to such interagency collaboration are critically examined for change as necessary to improve effectiveness. In doing so, the national security apparatus will gain the skills and flexibility that will not only prevent future terrorist attacks but might also help us recognize and counter the next adaptive threat on the horizon.

### Pre-9/11 Counterterrorism Intelligence Efforts

International terrorism is not a new national security problem for the United States. Its preeminence as an aspect of national security, though, has grown since the attacks of the 1990s that included the bombing the World Trade Center in 1993, the attack on the Khobar Towers in 1996, and the bombings of American embassies in Africa in 1998. In 1986, Benjamin Netanyahu wrote that the United States discovered terrorism in the mid-1960s; recognized itself as the primary target in the 1970s; and started thinking about action in the 1980s. He also identified communist totalitarianism and Islamic radicalism as the inspiration for most terrorism at the time. While the United States was certainly the target of terrorist attacks throughout the Cold War, the end of the Cold War gave way to an increase in frequency and lethality of terrorism by Islamic radical groups.<sup>1</sup>

Well before 9/11, the national intelligence community, including the Federal Bureau of Investigation (FBI), was monitoring terrorist network activity. Some analysts had already identified Osama bin Laden as a key player in international Islamic terrorism. Over the decades, the United States had employed the diplomatic and economic instruments of national power to the issue of international terrorism, and it had created and trained military forces capable of combating terrorists around the



world.<sup>2</sup> The Clinton Administration came to office as the nation was determining its peace dividend at the end of the Cold War, and consistent with a 1980s definition of terrorism as a crime, it treated terrorism largely as a law enforcement issue. The impact on the Department of Defense (DOD) was a perception that the tools of counterterrorism were arrests, extradition, and rendition, not military force. DOD provided transportation for Department of Justice (DOJ) operations with little complaint, as most senior DOD officials did not consider terrorism an imminent threat. The Clinton Administration had tough policy initiatives that included preemption and disruption of terrorist networks, as well as a Presidential finding after the bombings of 1998 that authorized the killing of Osama bin Laden and his senior lieutenants. The Administration seemed reluctant, however, to actually employ existing Special Operations forces and capabilities, undoubtedly influenced by the 1993 events in Mogadishu, Somalia.<sup>3</sup>

Intelligence reform is also not new. There were several investigations of the intelligence community to assess its adequacy and relevance for the needs of the post-Cold War world and the 21<sup>st</sup> century. Despite a history of asking hard questions and debating reform and integration, the latter years of the 20<sup>th</sup> century and early part of the 21<sup>st</sup> century saw only minor tweaks in the system. A study updated in 2004 chronicles the history of intelligence reform proposals, which typically aligned with trends in foreign policy and the general view of the international environment. This study also examines the numerous Legislative and Executive Branch investigations into the intelligence community since 1949. Of note, transnational terrorism was among the significant threats identified for the post-Cold War world. The Aspin-Brown Commission in 1995



and 1996 identified terrorism as global crime and gave it special attention as an intelligence problem; it was identified as a “paramount security concern.”<sup>4</sup>

In the pre-9/11 environment, the FBI, an agency of the DOJ, had a significant role in the nation’s counterterrorism effort and understood the criticality of timely and accurate information regarding terrorist activity.<sup>5</sup> The FBI conducted criminal investigations and intelligence investigations, and it could conduct the latter on suspected international terrorists even if there was no specific evidence of a terrorist act. Instead of prosecuting a suspect for a crime, the goal of such intelligence investigations was prevention of an attack.<sup>6</sup> Since 1983, the FBI had broad authorities to prevent terrorism and it gained additional capabilities after the attacks of the 1990s, including an increase in the number of agents working counterterrorism investigations.<sup>7</sup> William H. Webster, former Director of the FBI, identified the FBI as the principal organization responsible for international and domestic terrorism in the United States and highlighted its increased capabilities as the establishment of a research and analysis center within the headquarters; cooperation with other law enforcement agencies; the creation of several joint terrorism task forces in major cities; and the establishment of Hostage Rescue Teams (HRT). Though he also highlighted intelligence as a key capability that needed to improve in the fight against terrorism, he did not specifically mention collaboration with other members of the Intelligence Community.<sup>8</sup> Despite expanded authorities and capabilities, a key criticism of the 9/11 Commission was that the FBI was unable to connect the knowledge of its field agents with national priorities.<sup>9</sup> Some of this issue is traceable to remaining capability shortfalls in compatible information sharing systems, but a large part of the issue was also cultural



within the FBI and within the entire intelligence community. Within the FBI, the cultural preference still resided with the reactive criminal investigations and the work of field agents; intelligence analysts and their predictive efforts were given secondary consideration.<sup>10</sup> Within the intelligence community, the FBI generally sought to protect its case sensitive evidence, and other agencies sought to protect their sources, methods, information, and functional roles.

DOD intelligence, meanwhile, remained focused on support to forces in assigned regions and to specific missions such as the deployment to Somalia and later to Haiti. DOD struggled with its post-Cold War role, as did many other parts of the United States national security apparatus, but military intelligence remained primarily focused on the armed forces of known or potential adversaries around the world to support warfighters and planners, defense policy, and weapon systems acquisition programs. With the commitment of a large number of troops to peace enforcement operations in Bosnia beginning in 1995, DOD developed new structures and processes to deal with the demands of that mission, including the hunt for war criminals.<sup>11</sup> Counterterrorism did not garner considerable attention.

In a study and report that pre-dates 9/11, a survey of the national security environment included international terrorism as a transnational threat, also called global crime.<sup>12</sup> Transnational threats are defined by Title 50, United States Code as “any transnational activity, including international terrorism, narcotics trafficking, proliferation of weapons of mass destruction and delivery systems for such weapons, and organized crime, that threatens the national security of the United States.”<sup>13</sup> Such individuals or groups are not limited by government or national boundaries, and their activities often



overlap. Transnational threats are about moving people, drugs, weapons, and money across the globe in an illicit manner, and such activity creates opportunities for terrorists to exploit.<sup>14</sup> The problems of transnational threats cross many departments and agencies of government at several levels.

There are good reasons that have been generally accepted for separating law enforcement information and intelligence as a routine practice. Successful prosecutions in the realm of law enforcement require proof beyond a reasonable doubt as the standard in criminal court. When FBI agents operate in this capacity, they are seeking solid evidence and protection of a chain of custody. Intelligence has generally been kept separate from law enforcement to preserve the legal distinctions between foreign and domestic intelligence and to protect the rights of United States citizens. Military forces are generally prohibited by Posse Comitatus from conducting law enforcement operations, and discussions of collaboration can cause anxiety over crossing lines. Additionally, intelligence sources and methods should not be exposed in unclassified court proceedings. The expansion of terrorist activity over the years, though, has resulted in a trend of much of the activity of an indicted suspect actually occurring overseas. As terrorists adapt their tactics, government institutions need to consider what adaptations might be necessary to sustain effective counterterrorism efforts.

#### Post-9/11 Counterterrorism Intelligence Efforts

With the perspective of almost two more decades of hindsight, it appears that while the United States started thinking about action in the 1980s, it took a catastrophic attack on American soil for terrorism to grab the attention of the average citizen and to prompt a demand for action across all of government. The attacks of 1998, the attack



on the USS Cole in Yemen in 2000, and the devastating attacks of September 11, 2001 put Al Qaeda at the top of the list of enemies of the state, and fighting terrorism became a national priority for the United States. The demand for action and the Bush Administration's approach to terrorism as a war had important implications for how to proceed.

The Bush Administration's response to 9/11 was heavily dependent on intelligence. The objectives were to prevent the next attack, target terrorist networks and all aspects of their support, and disrupt networks abroad.<sup>15</sup> Declaring a war on terror, the Administration did not view terrorism as a law enforcement issue, and its interagency war on terrorism included a major role for DOD in hunting terrorists and gathering intelligence. The 9/11 Commission had identified barriers to collaboration within the intelligence community as the main fault line that led to 9/11, particularly between FBI and the rest of the intelligence community.<sup>16</sup> An important part of the solution is increased collaboration between the FBI (DOJ) and DOD, given that DOD has procedures and processes for more easily gaining access to the Central Intelligence Agency (CIA) and the rest of national intelligence community.

In the aftermath of the 9/11, the United States overhauled its national intelligence establishment and increased overall membership in the intelligence community, adding the United States Coast Guard (USCG) as well as the Offices of Intelligence and Analysis within the Department of Treasury (DOT) and the newly created Department of Homeland Security (DHS). The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the position of the Director of National Intelligence (DNI) to assume authority over all agencies of the intelligence community. Executive Order



13354 established a National Counterterrorism Center (NCTC) under the DNI to integrate intelligence regarding terrorist activity, to facilitate information sharing, and to ensure unity of effort. The NCTC replaced the Terrorism Threat Integration Center (TTIC) in 2004, and IRTPA codified its responsibilities. The Director of NCTC follows the policy direction of the President, the National Security Council, and the Homeland Security Council, and departments and agencies that participate in NCTC operations include the CIA, DHS, FBI, and DOD. Executive Order 13356 directed cooperation in intelligence collection, analysis, and information sharing.<sup>17</sup> A familiar theme for the post-9/11 iteration of intelligence reform was the need for greater cooperation and information sharing. There have since been several years of sorting through missions, roles, responsibilities, authorities, manning, and funding.

The FBI maintains the mission “to protect and defend the United States against terrorist and foreign intelligence threats” as well as to enforce criminal laws and provide criminal justice services to agencies and partners.<sup>18</sup> Counterterrorism is first among its national security priorities. Since 9/11, the FBI has expanded its intelligence capabilities and shifted resources from criminal investigations to terrorism investigations. It participates in several joint centers, including the NCTC and the Foreign Terrorist Tracking Task Force that includes CIA, Immigration and Customs Enforcement (ICE), and DOD. This task force seeks to keep terrorists and their supporters out of the United States or to use collective information to locate, remove, detain, or prosecute.<sup>19</sup> Responding to a Presidential directive, the FBI established a National Security Branch to integrate the FBI’s counterterrorism, counterintelligence, and intelligence efforts and improve predictive and preventive abilities.<sup>20</sup>



DOD had several responses to 9/11. The United States Special Operations Command (USSOCOM) became the DOD lead for synchronizing its global war on terror. Special Operations forces received a leading role in taking the fight to terrorists abroad. To address his intelligence concerns for the war on terror, the Secretary of Defense established the position of Undersecretary of Defense for Intelligence (USDI) and selected Stephen Cambone as the first Undersecretary. Given Secretary Rumsfeld's intent to give the Special Operations community a major role in the war on terror, it was not coincidental that the first Deputy Undersecretary of Defense for Intelligence, Lieutenant General William G. "Jerry" Boykin, has an extensive Special Operations background.<sup>21</sup> DOD also established U.S. Northern Command (USNORTHCOM) in 2002 and assigned it the mission "to provide command and control of DOD's homeland defense efforts and to coordinate defense support of civil authorities."<sup>22</sup> USNORTHCOM is DOD's lead for homeland defense and civil support. In defining its role, the command uses a spectrum of conflict that shows national security threats at one end and law enforcement or criminal threats at the other. The national security threats are the purview of DOD; the law enforcement or criminal threats are the purview of DOJ or DHS. There is a blurring of the line between national security and law enforcement threats, however, and the methods of addressing the transnational threats that operate across the spectrum often overlap. When they do, DOD can operate in support of lead federal agencies for civil support.<sup>23</sup>

It seems intuitive that the United States should approach counterterrorism as an interagency effort. Given the long-standing employment of the diplomatic and economic instrument and more recent use of financial controls and court actions, it is relatively



easy to argue that the United States has always done so.<sup>24</sup> The intelligence community, however, particularly the FBI and the CIA, received the brunt of the scrutiny and criticism for the failures that led to 9/11 and witnessed the most significant efforts at reform. The very nature of international terrorism as a transnational threat requires interagency collaboration, and a particularly valuable collaborative effort is between the DOJ-- through the FBI--and DOD. Both are members of the national intelligence community, but as previously discussed, collaboration within the community has been far from perfect. Although the barriers to FBI and DOD collaboration include both legal and practical measures, the value of collaboration for counterterrorism outweighs the risks. Law enforcement techniques and resources produce critical information about terrorist individuals and operations. Military intelligence, when targeting an individual or a network, also produces critical information. The combination of law enforcement and military intelligence capabilities provides a broader understanding of terrorist networks, capabilities, and intentions and offers opportunities for cueing of additional resources. Pre-9/11 intelligence reform proposals indicated this kind of collaboration was necessary, and the National Security Council in 1996 even had a committee on transnational threats to develop policies and procedures to facilitate such information sharing across federal departments.<sup>25</sup>

#### Case studies – Joint Task Force North; Special Operations; 1<sup>st</sup> Brigade

*Joint Task Force North.* Joint Task Force North (JTF-N) has a twenty year history of interagency intelligence collaboration. JTF-N is the USNORTHCOM organization tasked with providing DOD support to federal law enforcement agencies to identify and interdict transnational threat along the approaches to the United States homeland.



During the latter years of the Cold War, JTF-N was established as Joint Task Force Six (JTF-6) in 1989 in response to President George H. W. Bush's declaration of a war on drugs. The unit planned and coordinated DOD support for agencies along the southwest border to counter illegal drug trafficking. After 9/11 and the creation of USNORTHCOM in 2002, the Secretary of Defense directed that USNORTHCOM review the mission of JTF-6. In July 2004, USNORTHCOM directed JTF-6 to expand its area to include all of the approaches to the continental United States, not just the southwest border, and to expand its mission to include support for countering transnational threats. In September 2004, JTF-6 became JTF-N, and its mission statement highlights its inherent interagency perspective: "Joint Task Force North provides military support to law enforcement agencies, conducts theater security cooperation as directed, and facilitates interagency synchronization within the USNORTHCOM area of responsibility in order to anticipate, detect, deter, prevent, and defeat transnational threats to the homeland."<sup>26</sup> For JTF-N, transnational threats translate into drug trafficking organizations, alien smuggling organizations, and foreign terrorist opportunities.<sup>27</sup>

JTF-N provides four categories of military support to law enforcement agencies: operational, intelligence, engineer, and general.<sup>28</sup> Operational support really consists of intelligence, surveillance, and reconnaissance (ISR) support in the form of aviation reconnaissance or aviation with forward looking infrared radar (FLIR), unmanned aerial systems, aerial or maritime radars, and ground sensors. Most of these ISR capabilities are unique to DOD and therefore are an important complement to law enforcement capabilities. As law enforcement agencies acquire more of their own ISR systems, intelligence continues to be relevant as one of the most important categories of support



to law enforcement. DOD has well-established intelligence processes for collection, processing, and analysis of information and the development of intelligence products. Whereas law enforcement intelligence tends to be reactive and builds evidence for a case, military intelligence analysts try to be predictive through development of patterns of enemy activity. JTF-N analysts' efforts complement law enforcement efforts by providing a more comprehensive perspective of threat organizations and networks. Additionally, JTF-N analysts help law enforcement agencies identify critical gaps in their knowledge of a particular threat, develop a related and specific intelligence requirement, and access the national intelligence community for satisfaction of the requirement. Personnel from JTF-N's Intelligence Directorate developed a portal-based system to facilitate tracking of these intelligence collection requirements and associated responses to enable sharing with other interested agencies. Appreciating the need to preserve evidence for specific law enforcement cases, JTF-N analysts occasionally provide case-sensitive support that tailors collection or analysis and limits information distribution to the specific agency supported. Additionally, JTF-N analysts provide collaborative threat assessments, geospatial intelligence products, link analysis products, and routine collaboration.

For much of its history, JTF-N typically provided military support to a single agency at a time. Over the past few years, multi-sensor, multi-agency operations have become more common. These operations are the epitome of interagency collaboration and the blending of law enforcement and military intelligence capabilities. The intent of these operations is to provide the right mix of military intelligence capabilities to improve the situational awareness of participating law enforcement agencies and enhance their



ability to counter illicit transnational activity with decision quality information. They are operations to gain intelligence. Law enforcement agencies gain access to greater intelligence collection assets, particularly technical. DOD gains access to the intelligence collection resources of law enforcement, particularly in the realm of human intelligence, which can be more robust and offers a different perspective. A regional FBI unit reluctantly participated in one such operation in which the USCG was the lead federal agency. Participating agencies provided a range of intelligence capabilities and expertise about the operational area's illicit activity and potential terrorist networks and opportunities. After seeing the value in interagency intelligence sharing at that level, that FBI unit took the lead in a similar multi-sensor, multi-agency operation the following year. The relationships established during that operation continue to provide information sharing avenues that have resulted in impressive tangible results.

*Special Operations Forces Operations.* United States' Special Operations Forces (SOF) are arguably DOD's most experienced force at routine interagency operations, and law enforcement information informs many of their activities in fighting the global war on terror. Conversely, SOF operations outside the continental United States (OCONUS) yield information that becomes part of the base of knowledge that drives decisions for further military action or for law enforcement action.

Shortly after 9/11 but consistent with the pre-9/11 approach to terrorism as a national security issue, many Pentagon officials viewed the war on terror as largely a pursuit outside the military's purview, with emphasis on diplomatic, financial, economic, law enforcement, and intelligence activities.<sup>29</sup> Secretary of Defense Rumsfeld, however, immediately saw a role for SOF on a global scale. Targets would include terrorist



operators, their money, and their communications. He envisioned global pursuit and asked about places like South America and Mauritania in addition to Afghanistan. Secretary Rumsfeld's directives and policies for DOD's participation in the war on terror significantly expanded SOF capabilities and lethality in short order. He wanted to capture or kill terrorists, not arrest them, and those captured would be interrogated for information necessary to uncovering additional nodes and links in the network or to preventing any further attacks.<sup>30</sup> In some cases, SOF were already deployed and working with partner nations to develop their capabilities for combating terrorist and insurgent activities. Other forces deployed to Afghanistan in the fall of 2001 and began conducting operations with CIA teams and indigenous forces in theater.<sup>31</sup> SOF also had a major role in counterterrorist operations in Iraq from the beginning of Operation IRAQI FREEDOM, with task forces dedicated to locating and capturing or killing specific high value targets. By the summer of 2003, SOF operations that integrated conventional, allied, and interagency capabilities were deemed a success, and those operations have since had more than five years to mature.<sup>32</sup>

Since the beginning of Operations ENDURING FREEDOM and IRAQI FREEDOM, the United States has altered its strategies in Afghanistan and in Iraq, but SOF operations against terrorists and their networks continue in both countries. As the enemy has adapted to the presence and operations of coalition forces, SOF have adapted their practices to improve their ability to counter terrorists and prevent attacks, and intelligence is the primary focus. Within the SOF community, there has been a paradigm shift. No longer is intelligence primarily a staff function that supports operations; intelligence *is* operations. This is similar to the law enforcement technique of



gathering evidence, but the SOF community strives to prevent attacks instead of reacting to them. To gain actionable intelligence, units must take action and fight for knowledge across the force. Successful campaign plans, therefore, synchronize and integrate intelligence activities to achieve military objectives.<sup>33</sup>

The former Director of Intelligence for Joint Special Operations Command, Brigadier General Michael T. Flynn, echoes this transformation in the relationship between intelligence and operations that the SOF community led in the war on terror. He also describes a targeting model that encompasses the concept of intelligence as operations, that highlights the blending of law enforcement techniques with military intelligence capabilities, and that emphasizes the primacy of intelligence in the war on terror. The model is the Find, Fix, Finish, Exploit, Analyze or F3EA model.<sup>34</sup> See Figure 1. Success of the F3EA model relies on a combined arms team of operations and

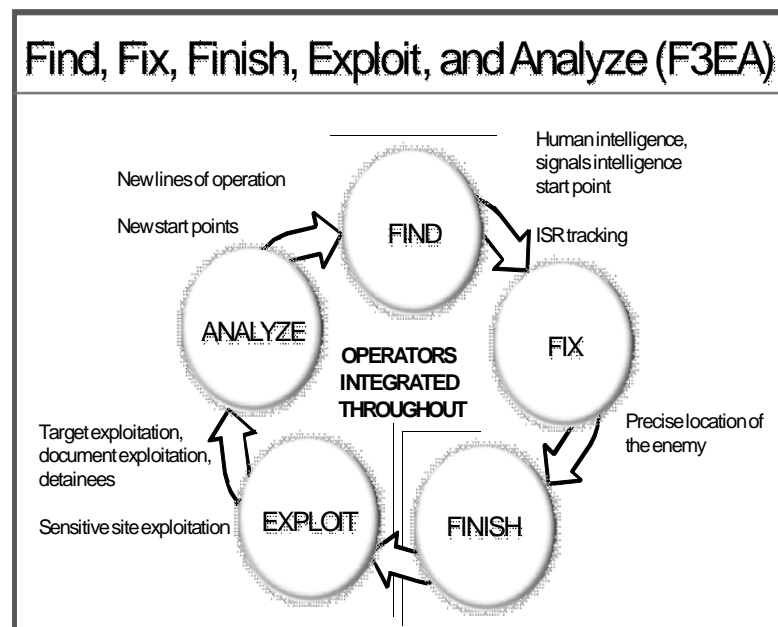


Figure 1: F3EA Targeting Model<sup>35</sup>



intelligence and focuses on intelligence as the most effective tool. SOF and ISR and other intelligence disciplines work under a single commander. Intelligence is from human collectors, detainees, signals intelligence platforms, and aerial surveillance systems and combines available law enforcement information with military intelligence as necessary to understand the target. This methodology also employs law enforcement techniques such as the persistent surveillance that resembles a stake-out and enables analysts to become intimately familiar with a target and his patterns. Detainee intelligence results from talking to network participants about the structure and leaders, operators, and facilitators much as a law enforcement official questions suspects. The preservation of captured material for exploitation is another law enforcement technique used to maximize the ability to execute the most important parts of the F3EA model, the exploitation and analysis that could lead to identification of subsequent targets. Documents, computers, cell phones and even pocket litter offer clues for networks, organizations, capabilities, and intentions.

*1<sup>st</sup> Brigade, 10<sup>th</sup> Mountain Division.* Conventional units that have conducted operations in Afghanistan or Iraq have also gained an appreciation for the value of DOJ and DOD collaboration to fight terrorism. A recent example of effective collaboration occurred in the 1<sup>st</sup> Brigade, 10<sup>th</sup> Mountain Division area of operations in Iraq. The brigade, part of Multinational Division-North, was responsible for the province of Kirkuk, a multiethnic region about fifty-five miles north of Baghdad. In a DOD news briefing from Iraq, Colonel David Paschal attributed the successful reduction of enemy activity in the province to several factors, first among them precision targeting of insurgent leadership.<sup>36</sup> The brigade had interagency representatives, including FBI and former FBI



agents, working within its area and with its soldiers specifically to assist with network defeat operations. These individuals brought subject matter expertise of the terrorists, but also of the nodes and links and activities within terrorist networks, and they worked with the brigade's intelligence and operations sections to develop as comprehensive a picture of a target network and its components as possible.

Law enforcement agents working with conventional brigade combat teams have also contributed to their increased proficiency at sensitive site exploitation (SSE) operations. Sensitive sites include suspected war crimes sites, weapons of mass destruction facilities, high value target facilities, or any other secretive sites an adversary uses. Ideally, specialized teams that include experts with such skills as forensics, technical intelligence, weapons expertise, and detainee questioning actually conduct the exploitation operations. Soldiers generally have security and support missions, and many understood their mission more clearly when a commander told them to replicate a forensics crime show from television.<sup>37</sup> The war on terror has called upon soldiers to conduct exploitation operations in the absence of subject matter experts or SOF, and their experience with law enforcement personnel has improved results and informed doctrine and evolving practices. The process of exploiting sites is critical to developing additional information to feed the intelligence and targeting processes.<sup>38</sup>

Colonel Paschal established a weekly schedule that included interagency assessment meetings at which the brigade intelligence staff, SOF personnel, FBI representatives and others discussed the intelligence perspective of the area. This included a discussion of high value targets and their status, as well as anticipated



reactions to any proposed brigade operations. For example, detaining a particular individual could empower and enable some part of local government to improve economic conditions. The interagency meetings provided the information that set the stage for subsequent lethal and nonlethal engagement or targeting meetings within the brigade.<sup>39</sup>

The precision targeting to which Colonel Paschal attributed the reduction of enemy activity was the result of blending law enforcement and military intelligence capabilities. When Colonel Paschal's brigade first arrived in Iraq in September 2007, their primary enemy was Al Qaeda in Iraq. In their targeting efforts, law enforcement skills contributed to solid data collection and exploitation, as well as a comprehensive understanding of a network to focus targeting efforts. Military intelligence capabilities enabled collection with technical and human resources; processing of all sources of information; and analysis of information and data to develop actionable intelligence. The brigade's routine collaboration with SOF further enhanced its knowledge and its capabilities. As Colonel Paschal's brigade killed or captured twenty high value targets, they identified and targeted others. By the end of 1<sup>st</sup> Brigade's tour, the enemy was a local derivative of Al Qaeda with much less effective leadership and operators. Precision targeting enabled the Brigade to conduct fewer cordon and search operations and to lower its profile throughout the province, which paid dividends with the local population. With fewer terrorist attacks occurring, they gained confidence in their own security forces and could see the results of Provincial Reconstruction Team efforts.



## Conclusion

In the fight against international terrorism, absolute security through intelligence is unrealistic; terrorists intentionally seek unpredictability and opportunities to exploit vulnerabilities. The collection capabilities of the intelligence community are not omnipresent, and its analysts are not omniscient. Regardless of how ambitious the goal of absolute security may be, it is one for which the United States must continue to strive. In pursuit of this goal, the blending of law enforcement and military intelligence capabilities goes a long way towards building the most comprehensive understanding possible of terrorist networks, capabilities, operations, and intentions. The case studies above illustrated effective blending of these capabilities over the past twenty years to address transnational threats to the United States and the subset of international terrorism. They highlighted the symbiotic relationship between the two communities and demonstrated the application to Special Operations and conventional military forces.

Interagency collaboration has become a popular concept in discussing national security concerns over the past several years. The proposal for greater collaboration between law enforcement and intelligence is certainly not a new one, but the mandate for doing so has perhaps never been clearer. International terrorism evolved as a major national security threat to the United States over several decades. A complex global network inflicted a catastrophic attack on the United States. Blending of law enforcement and military intelligence capabilities has proven effective in building decision quality intelligence to drive military action or law enforcement action.

There are certainly challenges in such close collaboration, initially stemming from organizational purposes. It is this difference in roles, however, that provides the complementary perspectives on the terrorist threat. Collaboration requires more



complicated oversight requirements, information sharing systems, information security practices, and processes to protect civil liberties of U.S. persons. Personnel and financial resource constraints complicate collaboration at some levels, despite good intentions. Finally, cultural barriers within organizations still hinder collaboration at all levels. The value of blending law enforcement and military intelligence capabilities warrants the effort to overcome these obstacles and to work to embed the best practices into institutional norms.

As the nation moves further away from the emotion of 9/11 and confronts the pressing concerns of a global economic crisis and a resurgence of operational focus in Afghanistan, it is important not to lose the lessons of the past eight years of the war on terror. The nature of the threat environment requires blending of best practices of law enforcement and military intelligence to gather, exploit, and analyze information to develop actionable intelligence to prevent terrorist attacks. The Obama Administration's agenda does include counterterrorism programs and initiatives that involve defeating terrorists worldwide and improving intelligence collection, analysis, and sharing capabilities. The agenda also includes an initiative to improve collaboration between U.S. and foreign intelligence and law enforcement.<sup>40</sup> If this initiative takes into account the insights from the case studies of JTF-N, SOF, and conventional brigades in the war on terror, there is reason for optimism. These insights suggest best practices for a way forward in balancing the right interagency capabilities to identify and counter the next emerging threat.



## Endnotes

<sup>1</sup> Benjamin Netanyahu, ed., *Terrorism: How the West Can Win* (New York: The Jonathan Institute, 1986), 225. This collection of essays based on an international conference held in 1984 highlights themes that are familiar in the current global war on terrorism: rule of law, Constitutional powers related to national security, tension between security and civil liberties, terrorists' goal of obtaining weapons of mass destruction, and the requirement for international cooperation to combat terrorism. It is also important to distinguish international terrorism from domestic terrorism; this paper focuses on international terrorism.

<sup>2</sup> William G. Boykin, *Never Surrender* (New York, NY: Faith Words, 2008). See also National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York, NY: Norton & Company, Inc., 2004), 98. Early Department of Defense counterterrorism measures were force protection, post-incident response, and hostage rescue.

<sup>3</sup> Richard Shultz, "Preempting Terrorists was not an Option: The Non-Use of SOF CT Units in the 1990s," briefing slides and notes, in *Rumsfeld's War: The Untold Story of America's Anti-Terror Commander*, Rowan Scarborough (Washington, DC: Regnery Publishers, Inc., 2004), 224-236. The briefing was one that Secretary of Defense Rumsfeld's staff requested to try to understand why the Clinton Administration never employed SOF to attack Osama bin Laden and Al Qaeda. Paul R. Pillar discusses pre-9/11 interagency efforts to counter terrorism, but also identifies law enforcement as the favored counterterrorism instrument of the past. Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington, DC: Brookings Institution, 2001).

<sup>4</sup> Commission on Roles and Capabilities of the United States Intelligence Community, "The Need for a Coordinated Response to Global Crime," in *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, DC: Government Printing Office, March 1, 1996), <http://www.fas.org/irp/commission/workplan.html> (accessed March 10, 2009).

<sup>5</sup> U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks* (Washington, DC: U.S. Government Printing Office, 2005), 8 <http://www.usdoj.gov/oig/special/0506/final.pdf> (accessed February 10, 2009).

<sup>6</sup> *Ibid.*, 9.

<sup>7</sup> Alan G. Theoharis, *The FBI and American Democracy* (Lawrence, KS: The University of Kansas Press, 2004), 1, 6-7, 149, 159-72.

<sup>8</sup> William H. Webster, "Fighting Terrorism in the United States" in *Terrorism: How the West Can Win*, ed. Benjamin Netanyahu (New York: The Jonathan Institute, 1986), 168-9.

<sup>9</sup> National Commission, *9/11 Commission Report*, 352.

<sup>10</sup> Richard A. Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the United States*, Congressional Research Services Report for Congress (Washington, DC: Library of Congress, January 16, 2001), 11 <http://www.loyola.edu/dept/politics/intel/CRS-RL30252.pdf> (accessed March 21, 2009).



<sup>11</sup> Kathleen A. Gavle, *Division Intelligence Requirements for Sustained Peace Enforcement Operations*, School of Advanced Military Studies Monograph (Fort Leavenworth, KS: Command and General Staff College, 2000). The greatest deficit in the force that proved essential to operations in the Balkans was in human intelligence and associated processing and analysis systems and structures.

<sup>12</sup> Commission on Roles and Capabilities, "The Need for a Coordinated Response to Global Crime."

<sup>13</sup> Cornell University Law School, Legal Information Institute, U.S. Code Collection, Title 50, Chapter 15, subchapter 1, section 402, National Security Council [http://www.law.cornell.edu/uscode/uscode50/usc\\_sec\\_50\\_00000402----000-.html](http://www.law.cornell.edu/uscode/uscode50/usc_sec_50_00000402----000-.html) (accessed March 20, 2009).

<sup>14</sup> COL Brian Lesieur, former J2, Joint Task Force North, discussion with author, November 2006. The concept of foreign terrorist opportunities was a key component of COL Lesieur's description of the transnational threat activity on which the Joint Task Force North Intelligence Directorate focused. It was a variation of the State Department's use of FTO to list foreign terrorist organizations. *U.S. Department of State Home Page, Foreign Terrorist Organizations Fact Sheet*, October 11, 2005, <http://www.state.gov/s/ct/rls/fs/37191.htm> (accessed March 18, 2009).

<sup>15</sup> Douglas J. Feith, *War and Decision: Inside the Pentagon at the Dawn of the War on Terror* (New York, NY: Harper Collins Publisher, 2008), ix, 9, 507. Two additional aspects of the Bush Administration's response included attention to terrorists' pursuit of weapons of mass destruction and emphasis on protecting the Constitution, civil liberties, and the American way of life.

<sup>16</sup> National Commission, *9/11 Commission Report*, 77, 89.

<sup>17</sup> *U.S. National Counterterrorism Center Home Page*, [http://www.nctc.gov/about\\_us/about\\_nctc.html](http://www.nctc.gov/about_us/about_nctc.html) (accessed March 4, 2009).

<sup>18</sup> *U.S. Federal Bureau of Investigation Home Page*, <http://www.fbi.gov/> (accessed March 4, 2009).

<sup>19</sup> *Ibid.*

<sup>20</sup> *Ibid.* See also Michael A. Turner, "Intelligence Reform and the Politics of Entrenchment," *International Journal of Intelligence and Counterintelligence*, 18, no. 3 (Spring 2005), 388-9. Intelligence reform has been the subject of many articles since 9/11, and critics argue the reforms have still been largely cosmetic. Detailed discussion of those reforms is beyond the scope of this project, and the reforms discussed simply frame the paper's arguments.

<sup>21</sup> Boykin, *Never Surrender*, 7-9.

<sup>22</sup> *U.S. Northern Command Home Page*, <http://www.usnorthcom.mil/About/index.html> (accessed March 4, 2009).

<sup>23</sup> *Ibid.* This discussion of the spectrum of threats is relevant to the first case study this paper provides. Joint Task Force North has operated for twenty years in the seam where threats converge and responses overlap.



<sup>24</sup> Pillar, *Terrorism and U.S. Foreign Policy*, xxix. He argues that the metaphor of a war is not helpful in that it discounts the many counterterrorism efforts that had been ongoing. He also suggests there has been a lot of continuity with interagency counterterrorism efforts and cautions against too much restructuring at the expense of getting things done.

<sup>25</sup> Richard A. Best, Jr., *Proposals for Intelligence Reform, 1949-2004*, Congressional Research Services Report for Congress (Washington, DC: Library of Congress, September 24, 2004), 2, 35, 38, <http://www.fas.org/irp/crs/RL32500.pdf> (accessed March 14, 2009). This report provides an historical survey of the proposals and is therefore a good source for trends and themes. It does illustrate the fact that many of the post-9/11 perspectives of the security environment and the intelligence apparatus required mirror those of previous commissions and investigations. Turner, "Intelligence Reform and Politics," 389.

<sup>26</sup> *Joint Task Force North Home Page*, command briefing slides, [http://www.jtfn.northcom.mil/factsheets/jtfn\\_brief.pdf](http://www.jtfn.northcom.mil/factsheets/jtfn_brief.pdf) (accessed February 20, 2009). The other two Joint Task Forces created for the war on drugs, JTF-4 and JTF-5, have since become Joint Interagency Task Force South (JIATF-S) and Joint Interagency Task Force –West (JIATF-W) and have retained their counterdrug mission. Establishing the focus for JTF-N efforts as the *approaches* to the continental United States provides a deeper look beyond the borders and involves using partner capacity and collaboration with Mexico and Canada. It also ensures that Department of Defense resources respect Posse Comitatus and intelligence oversight requirements.

<sup>27</sup> Much of the information for this case study comes from the author's experience as the Chief of the Joint Intelligence Support Element (JISE) of the Intelligence Directorate, 2006-2008. Although its mission statement encompasses transnational threats, JTF-N's authorities and funding still stem from counterdrug sources, so all operations must have a nexus to countering drug trafficking. Since drug trafficking networks provide opportunities for terrorists and insights into the illicit movement of weapons, drugs, people, and money, the requirement for a counterdrug nexus is not a significant restraint for most intelligence support. The intelligence aspect of the command's support to law enforcement is so significant, even in what is called the operational category, that the author suggested at one point the command could easily be a brigade-sized intelligence command. Many of the operational missions are typical of the kinds of operations military intelligence battalions and brigades conduct.

<sup>28</sup> *Joint Task Force North Home Page*. Engineer support typically consists of building or repairing roads or other infrastructure. General support consists of tunnel detection, mobile training teams, transportation, and sustainment.

<sup>29</sup> Feith, *War and Decision*, 86.

<sup>30</sup> Scarborough, *Rumsfeld's War*, 2-4, 21, 27.

<sup>31</sup> *Ibid.*, 22-25. Scarborough discusses SOF collaboration with the Central Intelligence Agency (CIA), but also with other nations. In particular, he reveals the work of the secretive Grey Fox unit in collecting specific intelligence on terrorist targets and then handing that information off to Jordanian and Thai officials for action.

<sup>32</sup> *Ibid.*, 27. The discussion is also based on author's experience in Operation IRAQI FREEDOM as the senior intelligence officer in 3<sup>rd</sup> Infantry Division's Division Tactical Command Post (DTAC).



<sup>33</sup> William G. Boykin, "Intelligence Support to Allied and Coalition Operations," briefing presented at the 16th Annual Special Operations/Low Intensity Conflict Symposium, February 2, 2005, <http://www.dtic.mil/ndia/2005solic/boykin.ppt> (accessed February 20, 2009). For the author and other intelligence professionals, the realization that intelligence is operations seems a little late in coming, but is understandably a recognition of the merging of other capabilities with those of intelligence operators. For those who have served as Operations Officers (S3) of military intelligence battalions or brigades, intelligence professionals have always conducted operations when deploying tactical or operational collection assets of any intelligence discipline. Experience with Joint Task Force North at Fort Bliss, Texas from 2006 to 2008 highlighted for the author that a considerable amount of the Department of Defense support that the unit provided to lead federal agencies in accordance with its authorities to do so consisted of conducting intelligence operations. Multiagency operations were often intelligence operations to gain better situational awareness of a particular operating environment and to improve targeting capability.

<sup>34</sup> Michael T. Flynn, Rich Juergens, and Thomas L. Cantrell, "Employing ISR: SOF Best Practices," *Joint Forces Quarterly*, no.50 (3rd quarter 2008) [http://www.ndu.edu/inss/Press/jfq\\_pages/editions/i50/15.pdf](http://www.ndu.edu/inss/Press/jfq_pages/editions/i50/15.pdf) (accessed February 20, 2009).

<sup>35</sup> Ibid.

<sup>36</sup> U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), *DOD News Briefing with COL Paschal from Iraq*, May 12, 2008, <http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=4228> (accessed March 21, 2009). The other factors to which COL Paschal attributed success were the increased capacity of the Iraqi security forces; the establishment of the Sons of Iraq and concerned citizens; and the Brigade's relationship with the Provincial Reconstruction Team led by Mr. Howard Keegan from the Department of State. COL Paschal had previously commanded a battalion in Afghanistan during Operation ENDURING FREEDOM. His battalion was the first to collocate and operate with a Provincial Reconstruction Team, and his insights from that experience served him well during operations in Iraq. Other information for this case study are from the author's interview with COL David Paschal, former Commander, 1<sup>st</sup> Brigade, 10<sup>th</sup> Mountain Division, March 21, 2009. He reinforced the value of interagency collaboration to counter terrorism and ultimately reduce the need for military operations to target terrorists in Iraq and Afghanistan. He also emphasized that despite continued professional military education and discussion of interagency and whole of government approaches to counterinsurgency and counterterrorism, officers across the force have not completely embraced this concept.

<sup>37</sup> U.S. Department of the Army, *Sensitive Site Operations*, Field Manual 3-90.15, (Washington, DC: U.S. Department of the Army, April 25, 2007), [https://www.akocomm.us.army.mil/usapa/doctrine/DR\\_pubs/dr\\_b/pdf/fm3\\_90x15.pdf](https://www.akocomm.us.army.mil/usapa/doctrine/DR_pubs/dr_b/pdf/fm3_90x15.pdf) (accessed March 20, 2009). Although such operations are not new in the U.S. Army, operations in the Balkans that required preservation of suspected war crimes sites and operations in the war on terror have provided many lessons and techniques that are captured in this doctrine. Additionally, Appendix B to this manual provides techniques for soldiers to use when law enforcement personnel are available.

<sup>38</sup> U.S. Department of the Army, *Sensitive Site Operations*, 2-11. Army Special Operations have significantly more detailed manuals that go into the specifics of forensics, and Special Forces intelligence soldiers are uniquely qualified and trained to be both combat soldiers and intelligence producing/gathering soldiers.



<sup>39</sup> These targeting meetings are similar to the nonlethal targeting operations that units conducted in Bosnia and Kosovo during Stabilization Force (SFOR) and Kosovo Force (KFOR) during the mid to late 1990s.

<sup>40</sup> *The White House Home Page*, [http://www.whitehouse.gov/agenda/homeland\\_security/](http://www.whitehouse.gov/agenda/homeland_security/) (accessed March 20, 2009). The initiative described is the Shared Security Partnership Program overseas.



